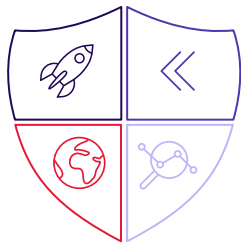# CGI AntiPhish

Ahead of the threat

CGI AntiPhish offers phishing prevention, neutralizing threats before they appear.

Unlike other phishing protection systems available on the market that react after threats reach their targets, CGI AntiPhish detects and neutralizes phishing long before an attack occurs. CGI has developed a tool that effectively neutralizes phishing's greatest advantage, its reliance on vulnerable human factors.

Holistic and Optimized

Retrospective Analysis

Real Time Analysis

Worldwide Reach

What is it?

Phishing Prevention Service

CGI AntiPhish is an automated service that scans public certificate data to detect newly created domains within minutes, identifying those designed for malicious impersonation.

It uses a robust and holistic analysis stack to verify domains and delivers results directly to the client. This enables automatic blocking and neutralization of malicious domains before an attack occurs, providing an additional layer of security for organizations.

Why?

Phishing is not only the most common cyberattack targeting organizations but also one of the most damaging, often leading to costly data breaches, financial losses, and reputational harm.

An organization's security is only as strong as its weakest link. Phishing preys on the human element. CGI AntiPhish is fully automated, stopping phishing threats before they reach their target and thus removing human error from the equation.
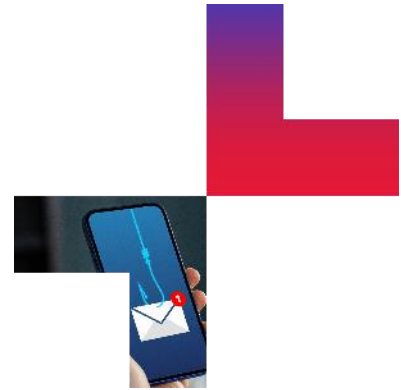
At least **one person** clicked a phishing link in around 86% of organizations

90% of corporate of security breaches are the result of phishing attacks

95% of attacks on business networks are the result of successful spear phishing

Preventing phishing may seem impossible, attackers rely on the element of surprise, hiding their websites until the moment of attack. But with CGI AntiPhish, there's no place for phishing to hide; new phishing websites are detected within mere minutes. By catching threats early, phishing can be neutralized before causing harm, prioritizing prevention over reaction.
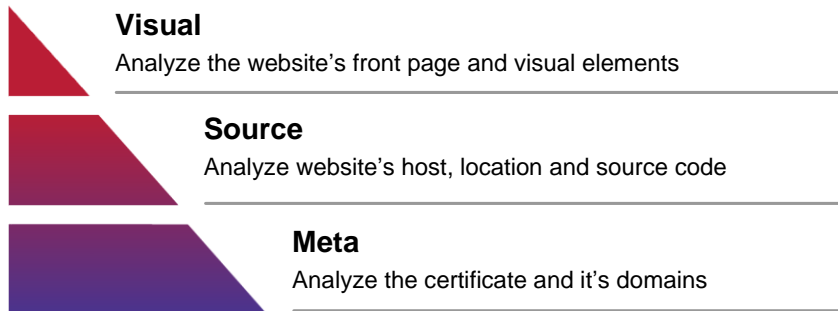
CGI AntiPhish

How?

CGI AntiPhish Methodology

CGI AntiPhish runs 24/7, continuously detecting, scanning and analyzing every newly registered website globally, identifying potential phishing threats in real-time.

CGI AntiPhish uses a modular and holistic stack of analysis steps to detect phishing impersonation websites;

Visual
Analyze the website's front page and visual elements

Source
Analyze website's host, location and source code
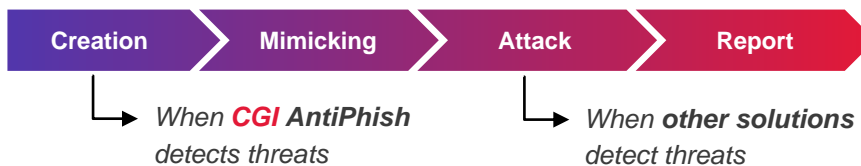
Meta
Analyze the certificate and it's domains

Once the analysis is complete, CGI AntiPhish identifies any website impersonating a legitimate organization and automatically sends it to your Intelligence Platform for internal neutralization. This information can also be used to issue an external Notice-and-Takedown.

What's new?

Preventing vs Protecting

The key difference between CGI AntiPhish and other phishing protection systems is that it does not just protect against possible attacks—it prevents them from happening in the first place.

Lifecycle of a **Phishing Website**

| Creation | Mimicking | Attack | Report |

*When **CGI** AntiPhish detects threats*

*When **other solutions** detect threats*

> Discover how CGI AntiPhish can add a preventive security layer to your organization. Contact us today for more information and a no-obligation, suitable demo:
>
> Contact: Gert Mariën
> Phone: +31 6 10236711
> Email: gert.marien@cgi.com

"Stay ahead of the threat with CGI AntiPhish, detecting and stopping attacks before reaching your organization."

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit cgi.com
Email us at info@cgi.com